Explotación Avanzada del Directorio Activo

Sandra Patricia Beltrán Ramírez

Trabajo de Grado presentado para optar al título de Especialista en Seguridad de la Información

Asesor: Nelson Augusto Forero Páez, PhD (c)

Ingeniero de Sistemas

Docente Ingeniería de Sistemas y Computación

Universidad Católica de Colombia

Facultad de Ingeniería

Especialización en Seguridad de la Información

Bogotá D.C., Colombia

2019

Dedicatoria

Dedico este proyecto de grado a mis familiares y amigos quienes fueron un gran apoyo emocional durante el tiempo en que desarrollaba esta investigación.

A la Universidad Católica de Colombia, donde desde su plataforma tecnológica y equipo docente, puso a nuestra disposición todo lo requerido para realizar un correcto desarrollo del proyecto.

A los tutores e Ingenieros Nelson Augusto Forero Páez y Sandra Milena Bernate quienes me brindaron la orientación desde sus conocimientos.

De igual manera agradezco a todas aquellas personas que de una u otra forma contribuyeron con la realización de este proyecto.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Los servidores, como sistemas informáticos que son, en donde también reposa la información del Directorio Activo, se encuentran expuestos a ataques informáticos provenientes de fuentes externas o internas, buscando con estos obtener información de las empresas provocando daños a corto, mediano y largo plazo.

Los hackers o ciberdelincuentes son personas que evaden los controles de seguridad y realizarn ataques logrando así su objetivo, por ello se propone en la presente investigación, la realización de un escaneo que permita identificar las posibles vulnerabilidades que se puedan presentar en el Directorio Activo.

Para realizar esta investigación se utilizó una máquina en Virtual box Kalli Linux, donde se instaló Nessus y Openvas y en Vmware un Server 2012R2, para realizar escaneos e identificar las vulnerabilidades. Se construyó un manual de buenas prácticas en el que se muestra la configuración del directorio activo con el fin de tener los mínimos riesgos de ataques informáticos.

Para lograr el desarrollo del proyecto se inició con la identificación de vulnerabilidades en el directorio activo, se ejecutaron herramientas para escanear desde Linux por red, documentando los hallazgos encontrados los cuales hacen parte del manual de buenas prácticas con el cual se pueden mitigar las vulnerabilidades

Palabras clave: Vulnerabilidad, hacker, directorio activo.

ABSTRACT

The servers as informatics system that they are, where is kept the information of the Active Directory, that are exposed to informatics attacks that proceed from external or internal sources, trying to obtain information from the companies with them, causing damages to short, medium and long term.

The hackers are people who avoid the security controls and make attacks reaching their objective, and that is the reason why in this investigation it is proposed the execution of an scanning that allow to identify the possible insecurities that can be presented in the Active Directory.

To make this investigation it was used a machine on Virtual Box Kalli Linux, in which were installed Nessus and Openvas and in VMware a Server 2012R2, to make scanning or identify the insecurities. It was built a manual of good practices in which is shown the configuration of the Active Directory with the propose of having minimum risks of informatics attacks.

To achieve the development of the project is was started with the identification of insecurities on the Active Directory, there were executed tools for scanning from Linux by network, documenting the findings found that are part of the manual of good practices which the one the insecurities can be reduced.

Keywords: insecurities, hackers, Active

I. INTRODUCCIÓN

En la actualidad el número de ataques cibernéticos a la seguridad de la información ha aumentado de forma proporcional al desarrollo de la tecnología, a pesar de los múltiples esfuerzos realizados por las empresas productoras de software, siguen existiendo un sin número de vulnerabilidades en los diferentes sistemas operativos que atentan contra la seguridad de la información y una de las formas de mitigarlos es realizando una revisión periódica de los sistemas de información

Los análisis de riesgos permiten tener una introducción y un enfoque aproximado a la investigación de éstos, en general conduce a la evaluación del impacto que cualquier violación de la seguridad podría tener en la empresa; muestra los riesgos existentes, identificando las amenazas que afectan al sistema informático; y determina la identificación de las vulnerabilidades del sistema a estas amenazas.

Dentro de los principios fundamentales en la seguridad informática, se encuentran, la Confidencialidad (entendida como la necesidad de que la información solo sea conocida por las personas autorizadas), la Integridad de la información (mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados), y la Disponibilidad de la información (La capacidad de permanecer accesible en el sitio, en el momento y en la forma en que los usuarios que estén autorizados lo requieran) [1], de acuerdo con estos principios el presente proyecto plantea como objetivo principal, identificar y evaluar las posibles vulnerabilidades, que atenten contra los principios de la seguridad informática en el Directorio Activo y así mismo plantear buenas prácticas y recomendaciones.

Teniendo en cuenta que existen muchas formas en las cuales un atacante puede obtener derechos de administrador de dominio en un Directorio Activo, el desarrollo de la presente investigación pretende describir algunos de los ataques existentes, pero poco conocidos, los cuales son omitidos en la creación de los directorios activos por parte de los administradores, quienes centran su atención en la creación de contraseñas seguras, permisos de usuario, etc, olvidando la importancia, en algunos casos por desconocimiento, de estas vulnerabilidades que pueden exponer la seguridad del Directorio Activo [2].

Sin desconocer la existencia de herramientas como el escaneo para detección de vulnerabilidades, resulta más efectivo para el administrador y más beneficioso en costos para la empresa, el poder descartar la mayor cantidad de riesgos desde su instalación.

Se espera lograr con la presente investigación que los administradores de red puedan tener una herramienta que facilite con la implementación de esta práctica, una óptima configuración del Directorio Activo, que beneficie a los usuarios, empresas y administradores en general.

II. GENERALIDADES

A. Línea de Investigación

Software inteligente y convergencia tecnológica.

B. Planteamiento del Problema

1) *Antecedentes del problema*

A partir de que Microsoft lanzara los roles y características de Directorio Activo en sus sistemas operativos de servidor, las empresas encontraron una herramienta de gestión que les permite asignar roles y responsables, asignar permisos, crear objetos como equipos, usuarios o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a una red y así mismo administrar las policitas dentro de la organización. Al tener una estructura jerárquica, que almacena información dentro de los objetos existentes en una red, permite métodos de almacenamiento de datos, y su disponibilidad para usuarios y administradores de red.

Teniendo en cuenta que esta estructura depende de protocolos de comunicación [3]tales como LDAP, DNS, DHCP, [4] etc. Su configuración básica ha presentado vulnerabilidades por diferentes motivos (configuración, parches de seguridad del sistema operativo) y algunos de estos han sido mitigados por Microsoft y otros a través de consultores especializados que mejoran día a día la configuración del directorio activo, Global Gate en su publicación virtual [5] nombra la existencia de un fallo o vulnerabilidad en Directorio Activo: “el fallo se debe a un error al comprobar el tamaño de un búfer asignado a la cadena "Server Name" que podría provocar un desbordamiento de memoria intermedia basada en heap 8 en el fichero mrxsmb.sys. Para llevar a cabo el ataque, se debe enviar un paquete de petición Browser Election al servidor SMB (de compartición de ficheros e impresoras) vulnerable. El exploit lo envía concretamente al puerto 138 sin necesidad de autenticación en un entorno de Directorio Activo. Por ahora el exploit permite provocar una denegación de servicio, pero parece ser posible modificarlo para conseguir ejecución de código. Microsoft no ha publicado "advisory" oficial y por supuesto, no existe parche oficial disponible.”

Lo anterior es solo un ejemplo de algunas fallas que se pueden presentar al realizar explotación del Directorio Activo, y ya que hasta la fecha no se ha dicho la última palabra, lo que se pretende es poder llegar a la máxima perfección en la configuración de éste, de modo que permita disminuir en un 80% las vulnerabilidades actuales.

Es tan amplio el estudio de vulnerabilidades del Directorio Activo, que actualmente ya existen empresas dedicadas exclusivamente a esta materia, es el caso de la empresa TRIMARC donde su Cofundador Sean Metcalf realiza investigaciones de vanguardia sobre ataques y actividades empresariales de Directorio Activo para identificar mejor cómo detectar, mitigar y prevenir ataques modernos.

2) ***Pregunta de investigación***

¿Cómo reducir el riesgo de amenaza interna a la disponibilidad, Confidencialidad e integridad del Directorio Activo en servidores con sistema operativo Windows Server 2012 R2, a partir de la implementación de buenas prácticas?

3) ***Variables del problema***

Al darse cuenta de la cantidad de vulnerabilidades presentadas en el Directorio Activo como lo son las que se evidencian en las contraseñas, la elevación de privilegios, políticas de grupo y controladores de dominio en las cuales se pueden presentar ataques al mismo, lo que se busca con las diferentes investigaciones y explotaciones al Directorio Activo, es reducir el porcentaje de ataques certeros.

Estos ataques pueden ser eficaces en la medida en que no se tengan los controles, no se sigan los protocolos y no se realicen las actualizaciones liberadas por el fabricante. Lo anterior se podría minimizar al realizar una configuración guiada por el Manual de Buenas Prácticas en la Configuración de Directorio Activo.

Riesgos: Uno de los mayores riesgos en cualquier ataque cibernético, es sin duda la perdida de información. Cuando uno de estos ataques ocurre al Directorio Activo de una empresa, el daño

puede ser irreversible si no se cuenta con copias de respaldo. El Directorio Activo vulnerable es la puerta de entrada a toda la información sensible de la organización ya que allí reposan los registros de usuario, contraseñas que van a ser el camino directo a toda la información financiera, tributaria y confidencial de la empresa.

4) *Justificación*

En los últimos años los ciberataques a las empresas han aumentado y cada día son más sofisticados y desarrollados, llevando a las organizaciones a altos costos por implementaciones de seguridad de última hora, lo anterior debido a que a pesar de que se vienen implementando controles y las empresas cada día manejan mejor sus filtros en lo que tiene que ver con seguridad informática, al no tener un 100% de seguridad, abre una pequeña puerta a los ataques cibernéticos, los cuales aprovechan cualquier falla para realizar estas acciones.

Sobre los ataques a Directorio Activo en Windows Server 2012R2, la compañía Microsoft ha venido trabajando desde hace mucho tiempo, logrando identificar aquellos que podrían ser más perjudiciales y publicando por su parte, parches de seguridad y actualizaciones que pueden descargarse desde la nube sin costo para el usuario con el fin de mitigar dichos ataques.

En Colombia, se puede destacar la evolución que ha tenido la legislación en esta materia, la cual se puede ver reflejada en una regulación más estricta hacia los delitos informáticos como es la Ley 1273 de 2009, la cual modifica el código penal, en Colombia, Microsoft Directorio Activo (AD) es un objetivo prioritario para los atacantes debido a su importancia en la autenticación y la autorización para todos los usuarios, por ello la condición de que Colombia cada día este más a la vanguardia en temas tecnológicos y de manejos de información por medios electrónicos debería alertar sobre una necesidad de aumentar en la misma medida los controles en seguridad informática para minimizar las posibilidades de riesgo.

Una noticia del Periódico El Tiempo revela cifras de ataques cibernéticos: “Ni las grandes organizaciones ni las empresas, ni los gobiernos ni los ciudadanos del común. Nadie está exento de ser víctima de un ciberataque. Al contrario, las amenazas cada día aumentan; solo en el último año (desde agosto del 2016 hasta el mismo mes de este año) se han presentado un total de 198

millones de ataques, según lo revela un informe de la firma de ciberseguridad Digiware. De acuerdo con la compañía, diariamente se registran en promedio 542.465 incidentes y el impacto de los delitos informáticos ha generado pérdidas por 6.179 millones de dólares en el país.
Recientemente, la compañía rusa Kaspersky también presentó un panorama regional del cibercrimen e informó que entre el primero de enero y el 31 de agosto del 2017 se han registrado un total de 677 millones de amenazas cibernéticas en América Latina. Esto quiere decir que cada hora hay 117 ataques y en un segundo se cometen 33. El sector financiero es el más afectado por los delitos informáticos en el país, con 214.600 ataques por día, según Digiware, seguido de telecomunicaciones, con 138.329; Gobierno, con 83.756 e industria, con 51.263 casos." [6]

Colombia, el país de Latinoamérica más afectado por ransomware en 2018, según Eset (Empresa de Seguridad Informática), se detectó un incremento del 199 por ciento respecto a las detecciones de ransomware durante 2017. [7, 6]

En este tipo de ataques, el abuso de Powershell, un lenguaje de scripting que todavía usan muchas empresas, ha sido una de las técnicas más utilizadas y ha supuesto un 26% de los bloqueos registrados. [8]

Como se puede evidenciar las anteriores estadísticas muestran como viene en incremento el índice de ataques, a raíz del crecimiento de la población que utiliza estos recursos informáticos, dentro de estos la implementación de Directorio Activo que es un blanco favorito para los atacantes por contener información de usuarios y permisos dentro de la red local de la compañía, puerta por la cual tendrían un fácil acceso a toda la información sensible de la misma. Por ende se requiere que las empresas realicen una configuración más detallada y orientada a preveer ataques aprovechando al máximo las utilidades que trae Microsoft como PsExec de la Suite Systernals y detectar intrusiones al Directorio Activo con la Herramienta PowerView incluida en el Framework de PowerShell para test de intrusión y otras herramientas las cuales van a ser utilizadas en esta investigación para una mejor configuración y robustez del Directorio Activo, teniendo en cuenta la necesidad a nivel de red local de lograr la identificación de cuál es la óptima seguridad que se debe implementar en las relaciones entre los usuarios, grupos y hosts del Directorio Activo.

A pesar de que, con el Boom de seguridad informática, se han minimizado los ataques, esta situación sigue siendo una problemática real en todos los escenarios tanto académicos como laborales que deben seguir trabajando cada día con el fin de minimizar los riesgos y crear conciencia a todo nivel que la primera seguridad que se debe ejercer es el control por parte de cada usuario.

III. OBJETIVOS

A. *Objetivo general*

Minimizar las brechas de seguridad en la configuración del Directorio Activo para servidores con Windows Server 2012 R2, a partir de la ejecución de comandos de cifrado, para identificar y reducir riesgos, en un ambiente de prueba con el fin de generar un instrumento basado en buenas prácticas para administradores de red.

B. *Objetivos específicos*

- Encontrar con la ejecución de los comandos de cifrado de Microsoft y las herramientas de escaneo Nessus y Open Vas , las posibles vulnerabilidades del Directorio Activo.

- Analizar las diferencias en un ambiente de prueba sobre una máquina con configuración básica y sobre una máquina con configuración segura de un Directorio Activo, para estudiar la reducción de las brechas de seguridad.

- Establecer condiciones ideales de configuración segura para el Directorio Activo, a través de las pruebas realizadas y que será socializado mediante un manual de buenas prácticas.

IV. MARCOS DE REFERENCIA

1) *Marco conceptual*

Los servidores requieren un sistema operativo específico para realizar la administración de usuarios y permisos, uno de ellos, objeto de estudio de la presente investigación es Windows Server 2012R2 [9] que contiene una herramienta de Directorio Activo, la cual es la encargada de dicha administración, que es la encargada de realizar esta acción (la administración de usuarios), definiendo sus permisos de acuerdo con los roles establecidos. La óptima configuración de éstos permite reducir las brechas de seguridad, que corresponden a incidentes que se ocasionan debido a una configuración básica, generando riesgos que son aquellos que podrían tener una repercusión en el cumplimiento de los objetivos organizacionales en materia de seguridad informática, debido a la explotación de vulnerabilidades (debilidades del sistema) y materialización de amenazas (cuando se explota la vulnerabilidad).

Existen certificaciones propuestas por Microsoft las cuales se basan en la completa configuración de Windows server 2012 R2 con todos sus servicios, roles, características, creaciones de políticas, instalación y administración del Directorio Activo siendo esta certificación de gran ayuda para los administradores de red para lo cual se debe tener en cuenta la seguridad en toda la configuración desde ceros para evitar amenazas a futuro. [10]

2) *Vulnerabilidad*

Se define como una falla o debilidad en los procedimientos, el diseño, la implementación o los controles internos de seguridad del sistema. La vulnerabilidad puede activarse accidentalmente o explotarse intencionalmente, causando violaciones de seguridad. [11]

Las vulnerabilidades se dividen en las siguientes tres categorías:

- Vulnerabilidades de tecnología / software
- Vulnerabilidades de configuración / interfaz web
- Vulnerabilidades de política de red / seguridad

3) ***Bases de datos de vulnerabilidades***

Existen diferentes bases de datos y repositorios de vulnerabilidades dentro de las cuales están:

- National Vulnerability Database (NVD) es un repositorio de gestión de vulnerabilidades que contiene fallas de software relacionadas con la seguridad y métricas de impacto. Numerosas bases de datos en línea están disponibles en Internet y exponen innumerables vulnerabilidades en diferentes tipos de productos, incluidos hardware y software.
- Computer Emergency Readiness Team (CERT) es otra base de datos de vulnerabilidades que proporciona información sobre vulnerabilidades de software. Los boletines de seguridad de Microsoft también están relacionados con problemas de seguridad descubiertos en el software de Microsoft, publicado por el Centro de respuesta de seguridad de Microsoft (MSRC).
- Common Vulnerabilities and Exposures (CVE) es otra lista de vulnerabilidades de la base de datos con un número de identificación.

La base de datos de vulnerabilidades de código abierto (OSVDB) proporciona información precisa e imparcial sobre vulnerabilidades de seguridad*.*

CVE determina vulnerabilidades inequívocamente por números CVE como CVE –2017–3161. El conjunto central en estos números indica el año de descubrimiento, mientras que el último conjunto indica un número AN que varía de uno a cualquiera, que comienza en uno cada año y se incrementa en uno por cada vulnerabilidad reportable [12].

El CWD ID – 79 (ID de enumeración de debilidad común) identifica de forma exclusiva este tipo de vulnerabilidad, como la secuencia de comandos entre sitios (XSS). La vulnerabilidad recientemente informada se agrega a la base de datos CVE después de seguir algunos pasos del procedimiento antes de mostrarse públicamente, que es controlada por una organización llamada MITRE. Según los registros de la base de datos CVE de los últimos nueve años, la Apache Software Foundation detectó e informó varias vulnerabilidades en sus productos, pero en el año actual 2019 hasta la fecha se han detectado un total de 49 vulnerabilidades de las 14 relacionadas con XSS y un DoS.

Según los datos disponibles en la base de datos CVE, las interfaces web son las más vulnerables. Casi todas las vulnerabilidades detectadas están parcheadas, pero algunas de ellas son explotadas por los atacantes con DoS, XSS, y obtienen acceso al sistema

4) ***Confidencialidad:***

Cuando se refiere a este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original. Por lo tanto lo que se pretende con este concepto es garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos a través de redes de comunicaciones. [13]

5) ***Control de acceso:***

El control de acceso se ejecuta acorde a los niveles de seguridad y es puesto en marcha por medio de la administración de la red. En su ejecución se da la aprobación de acceso a un sistema informático. Aquí el sistema verifica si concede o niega la petición de acceso del usuario, luego de verificar si las credenciales recibidas son las correctas y de acuerdo con su rol, si tiene los permisos de acceder en el sistema. Lo anterior de acuerdo con las políticas de control de acceso de una organización y/o aplicación web. [14]

6) ***Disponibilidad:***

Siendo uno de los principios básicos de la seguridad informática la disponibilidad del sistema informático también es un servicio de vital importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto para que las personas que van a acceder a la información sean solamente las interesadas [14]

7) ***Servidor***:

El concepto de servidor se aplica de forma genérica a equipos informáticos que suministran servicios de base de datos. ***[15]***

8) ***Windows server 2012 R2:***

Microsoft con la evolución de sus productos luego de la versión Windows Server R1 llega R2 siendo una plataforma flexible cada vez más exigente con tendencia a la virtualización, llega con nuevas funcionalidades útiles y prácticas que permiten basar el conjunto de Sistemas de información en una solución Microsoft.

Dentro de sus versiones se encuentran Datacenter, Estándar, Essentials y Foundation; ("Windows Server 2012 – Nuevo Licenciamiento", 2017) [16]

9) ***Bosque:***

En el Directorio Activo el bosque (forest) es una colección de uno o más dominios que comparten una misma estructura lógica, catálogo global, esquema y configuración.
Todos los dominios del bosque cuentan con relaciones de confianza automáticas de 2 vías y transitivas. El bosque representa una instancia completa del directorio y una frontera de seguridad. [17]

10) ***Árbol***

Un árbol es un grupo de dominios. Los dominios dentro de un árbol comparten el mismo espacio de nombre raíz, pero, a pesar de ello, los árboles no son límites de seguridad o replicación. [18]

11) ***Dominio***

Cada bosque contiene un dominio raíz. Se pueden usar dominios adicionales para crear más particiones dentro de un bosque. El propósito de un dominio es dividir el directorio en partes más pequeñas para poder controlar la replicación. Un dominio limita la replicación de Active Directory solo a los otros controladores de dominio que se encuentran en su interior. Por ejemplo: si tenemos dos oficinas, una Bogotá y otra en Medellín, la primera no debe replicar los datos de AD de la segunda y viceversa. De este modo, podemos ahorrar ancho de banda y limitar el daño causado a través de las brechas de seguridad. [19]

Cada controlador de un dominio contiene una copia idéntica de la base de datos de Active Directory de ese dominio por ejemplo sbeltran.com. De este modo se mantiene todo actualizado a través de la replicación constante.

A pesar de que los dominios se usaban en el modelo anterior, basado en Windows-NT, y aún proporcionan una barrera de seguridad, se recomienda que no sean solo los dominios los que se encarguen de controlar la replicación, sino que se empleen también las unidades organizativas (OU) para agrupar y limitar los permisos de seguridad.

12) ***Unidades Organizativas (OU)***

Una unidad organizativa permite agrupar la autoridad sobre un subconjunto de recursos de un dominio. Una OU proporciona un límite de seguridad para privilegios y autorización elevados, pero no limita la replicación de objetos de AD.

Las unidades organizativas se utilizan para delegar el control dentro de agrupaciones funcionales. Se deben usar las unidades organizativas para implementar y limitar la seguridad y los roles entre los grupos, mientras que los dominios deben usarse para controlar la replicación de Active Directory. [20]

C. ***Marco teórico***

ESTADO DEL ARTE DE LA SEGURIDAD EN DIRECTORIO ACTIVO

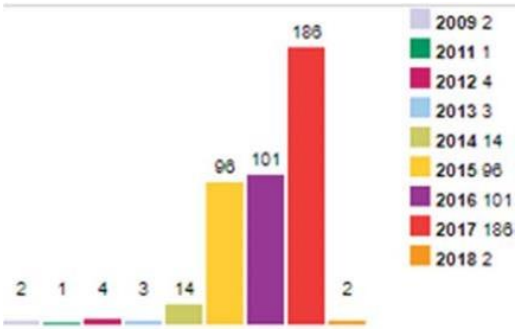

Figura 1. análisis de vulnerabilidades por año

Mencionado en https://www.cvedetails.com/version/121761/MicrosoftWindows-Server-2008-.html.

La figura 1 muestra que las vulnerabilidades de explotación aumentan con el tiempo, según se aplica al año 2017. De las figuras 2 y 3, la cantidad de vulnerabilidades es 186 y el tipo más común de vulnerabilidad en Windows Server 2008 es obtener información y obtener privilegios en Windows Server 2012.

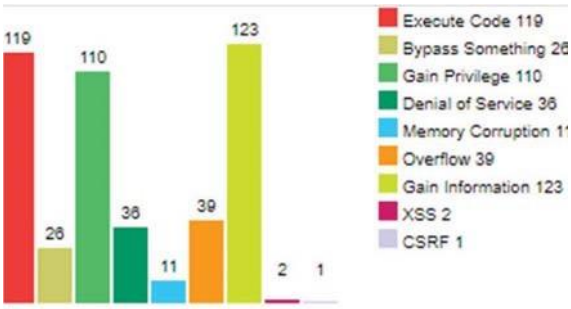

Figura 2. Análisis de vulnerabilidades

Mencionado en https://www.cvedetails.com/version/121761/MicrosoftWindows-Server-2008-.html

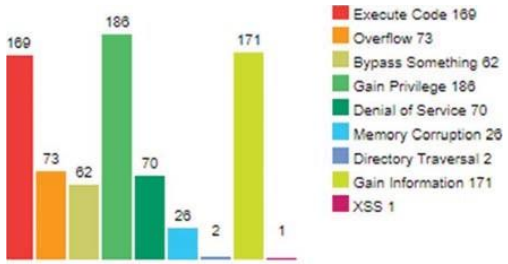

Figura 3. Análisis de vulnerabilidades

Mencionado en https://www.cvedetails.com/version/121761/MicrosoftWindows-Server-2008-.html

En la figura 2, muestra las otras vulnerabilidades que afectan al directorio activo, como la vulnerabilidad de scripting entre sitios (XSS) en los Servicios de certificados de Active Directory. Las secuencias de comandos entre sitios existen en Microsoft Windows Server 2003 SP2 y Server 2008 Gold, SP2, R2 y R2 SP1.La secuencia de comandos entre sitios ocurre cuando el atacante inyecta un código de secuencia de comandos web. El atacante puede explotar esta vulnerabilidad enviando al cliente / usuario un enlace y hacer que visite el sitio web vulnerable haciendo clic en el enlace. La segunda vulnerabilidad que afecta a Microsoft Active Directory es un desbordamiento de búfer. Esta vulnerabilidad puede permitir a los atacantes ejecutar código arbitrario con privilegios de servicio de red. Cuando el atacante no explota la vulnerabilidad de secuencias de comandos entre sitios, provocará una denegación de servicio y puede ocurrir en Microsoft Windows XP SP2 y SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2 y R2 SP1 y Windows 7 Gold y SP1 [21]

En los últimos años el boom de la seguridad informática ha generado un interés especial en la opinión pública y en un nivel más profundo en los gerentes y propietarios de empresa debido a los ataques informáticos. En el caso específico de Colombia los más comunes según información

de la Fiscalía son: Concierto para delinquir, hurto por medios informáticos, acceso abusivo al sistema informático, violación de datos personales, daño informático, transferencia no consentida de activos y uso de software malicioso. [22]

Para ello se vienen especializando cada vez más los profesionales en el área de seguridad informática y con el fin de responder a las necesidades de los grupos de interés, beneficiando y ampliando la oferta tanto educativa como laboral, ya que a nivel mundial son más las personas que buscan la protección de la información no solo la que se encuentra en sus servidores o en la nube, sino también de aquella que puede transmitirse mediante correos electrónicos, medios de almacenamiento como discos extraíbles, usb, entre otros. Una de las técnicas utilizadas por los profesionales de ciberdefensa (expertos en temas de seguridad informática) es aquella que se realiza a través de la ejecución de comandos, como Power SPloit el cual es un test de intrusión para encontrar la mayor cantidad de vulnerabilidades posibles en el Directorio Activo, y con una óptima configuración tener el menor riesgo posible tanto para la empresa como para los usuarios.

Los atacantes que se entrometen en la red de una organización intentan obtener privilegios de administrador de dominio de alguna manera (por ejemplo, escalada de privilegios, abuso de credenciales) y luego atacan al controlador de dominio para crear un ticket. Los atacantes que crean con éxito el Ticket pueden disfrazarse de cuentas de administrador arbitrarias cuando interfieren en el sistema. El límite de vencimiento extendido del Golden Ticket permite a los atacantes usarlo continuamente incluso después de cambiar la contraseña de la cuenta comprometida. Además, si los atacantes usan el Golden Ticket con una cuenta legítima, a menudo es difícil diferenciar los ataques maliciosos de las autenticaciones normales. [23]

La constante innovación de las últimas décadas, producto de los avances tecnológicos a nivel de sistemas de información tanto empresariales como personales, ha permitido numerosas ventajas para los usuarios en diferentes contextos, lo cual a su vez por el desconocimiento de protocolos de seguridad informática ha traído consigo una problemática que afecta a miles de personas a diario, los ataques a la seguridad informática en los sistemas de información, sean físicos o lógicos.

Siendo la información uno de los activos más importantes para una organización o usuario común, es un elemento que debe contar con todas las garantías de seguridad necesarias, los administradores de una red de datos incluyendo el Directorio Activo, deben establecer los

parámetros de configuración acordes con las políticas de seguridad de la organización, que a su vez deben cumplir con estándares de seguridad a nivel local e internacional. Cuando los sistemas y los datos se presentan en el Directorio Activo sin propietarios designados, propietarios de empresas y propietarios de TI, no existe ninguna cadena de responsabilidad para el suministro, administración, supervisión y actualización del sistema.

Esto trae como resultado infraestructuras débiles en las organizaciones expuestas a todo riesgo. Independientemente de las medidas de seguridad implementadas, no se puede garantizar ésta en un 100%. Por lo tanto, se requiere realizar una retroalimentación periódica que permita conocer las nuevas tendencias en ataques informáticos y de esta forma asegurar la información de cara a posibles eventualidades. Aquellas empresas que deciden contratar servicios para seguridad informática por una sola vez sin realizar procesos de mejora continua, están incurriendo en un desperdicio de recursos innecesario, ya que esta protección podría ser efectiva solo por un corto periodo de tiempo.

Hoy en día las organizaciones por desconocimiento asumen que una configuración básica de Directorio Activo podría ser aquella en la que las contraseñas de administradores y usuarios tengan cierta complejidad (mayúsculas, minúsculas, números y caracteres especiales) siendo un error ya que los datos de contraseña de las credenciales se pueden revertir fácilmente, convirtiéndolos en posibles víctimas de ataques informáticos, lo cual expondría la confidencialidad y calidad en el procesamiento de la información externa e interna. Es por ello que reviste importancia que la alta gerencia conozca el coste económico que podría conllevar a asumir las consecuencias de un ataque informático. Una mínima inversión en un sistema de información seguro, llevaría a un riesgo que se traduciría no solo en una nueva pérdida económica al intentar contrarrestar un ataque sino a atentar contra los tres principios fundamentales de la información, como son integridad, confidencialidad y disponibilidad. Cuando se presenta un ataque informático, este no puede ser atendido de manera aislada, por ejemplo: Si el ataque se evidencia en Directorio Activo, se debe no solo revisar las vulnerabilidades y posibles ataques a este sino también revisar las actualizaciones del servidor, y no dejar ningún detalle por revisar para evitar la propagación del ataque a otros servicios. En el ámbito empresarial, se puede contar con una estructura robusta de seguridad informática en una empresa, pero si no se tiene una disposición apropiada por parte de la alta gerencia y no se cuenta con una cultura de buenas prácticas por parte de los usuarios, será imposible alcanzar las metas de seguridad informática al

implementar su estructura de protección. La estructura de seguridad informática tiene como fin ofrecer protección tanto al software, como al hardware y a la información. Hacia allí deben encaminarse todas las acciones, la cuales permitirán fortalecer el sistema informático y obtener los resultados deseados, evitando al máximo un ataque, algunas de las recomendaciones podrían ser:

Permisos: No todos los usuarios deben tener permiso de administrador local (el cual tiene todos los permisos en la maquina local). Desde el Servicio de Directorio Activo podemos crear diferentes GPO (Políticas de grupo), una de ellas es configurando algunas acciones de restricción en la maquina local, por ejemplo:

a) El usuario tiene permisos solamente en los grupos globales en el directorio.

b) La contraseña de la cuenta administrador local es definida desde políticas de dominio y el usuario la desconoce.

Restricción de ejecución de aplicaciones: Con el lanzamiento de MS Windows 7 / 2012 R2, fue la aparición del APPLOCKER la cual puede administrarse perfectamente por GPO, permite al administrador de la plataforma definir que aplicaciones pueden usarse en cada equipo, independiente del software instalado en la máquina. Se pueden definir en la GPO que puede ejecutar dicho usuario, teniendo en cuenta los siguientes puntos:

a) Hacer un estudio por perfiles, de que aplicaciones requieren ejecutar los diferentes usuarios.

b) Establecer el software de la compañía (Se debe tener un catálogo de software validados por la empresa). Con esta herramienta el administrador tendrá la seguridad de que solo se utilizaran los programas licenciados o adquiridos por la empresa.

c) Los usuarios no deben ser administradores locales, pero si podrán tener los permisos para ejecutar las aplicaciones a las que se le otorgo acceso.

d) Auditoria del sistema

El administrador puede generar una Política de Grupo con el fin de auditar el comportamiento del usuario en la máquina, la cual le permitirá observar si existe un intento de ejecución de software malicioso, con el fin de tomar las acciones que correspondan.

La Figura 4 es un ejemplo ilustrativo de cómo un proceso "Kerberos", una variante del dominio

AD, funciona e interactúa con las cuentas intra-net. El proceso sigue los siguientes pasos [24]

ETAPA		PASO	
1	El intercambio de servicios de autenticación	**1**	Solicitud de servicio de autenticación Kerberos (KRB AS REQ)
		2	Respuesta del servicio de autenticación Kerberos (KRB AS REP)
2	El intercambio de servicios de otorgamiento de	**3**	Solicitud de servicio de concesión de tickets Kerberos (KRB TGS REQ)
		4	Kerberos ticket-granting service response (KRB TGS REP)
3	El intercambio cliente / servidor	**5**	Solicitud del servidor de aplicaciones Kerberos (KRB AP REQ)
		6	Respuesta del servidor de aplicaciones Kerberos (opcional) (KRB AP REP)

Tabla 1. Proceso kerberos

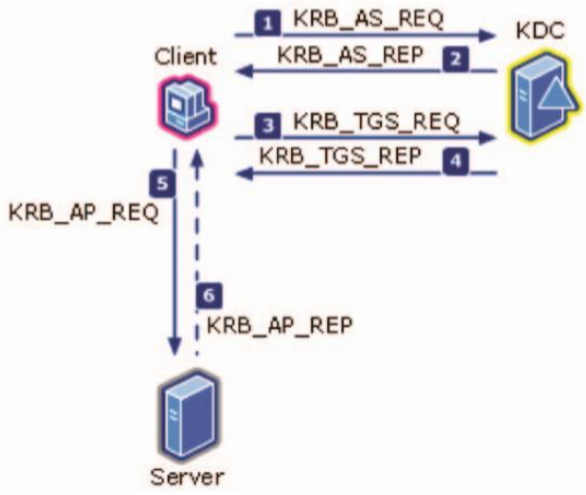

Figura 4. Una ilustración del controlador de dominio AD funciona e interactúa con cuentas intranet

Fuente:Arquitectura Active Directory [25]

Siendo Kerberos (protocolo de autenticación predeterminado de Windows) este permite verificar si la combinación de usuario y contraseña durante un intento de conexión al dominio es correcta, como se evidencia en la Figura 4, él se emplea por medio de tickets y un proceso de intercambio

de claves secretas de autenticación protegidas con encriptación simétrica.

V. METODOLOGÍA

A. Fases del trabajo de grado

El desarrollo de este proyecto se realiza en dos fases, las cuales garantizan el cumplimiento de los objetivos planteados, a través de la siguiente metodología descrita:

Fase 1: Identificación de las vulnerabilidades del servidor

Para ello se realizará la configuración del Windows Server 2012 R2 en un ambiente prueba sobre dos máquinas virtuales de VirtualBox, una en la cual se establecerá una configuración básica del Directorio Activo con modificaciones en la configuración de los usuarios y grupos, donde se identificarán vulnerabilidades con las herramientas de escaneo y la otra en donde se podrá evidenciar la configuración recomendada. Una vez estén listas se realizará un análisis de vulnerabilidades para identificar las deficiencias en la configuración que ponen en peligro la información, así mismo se realizará un análisis de riesgos con el fin de identificar las buenas prácticas que los reducen.

Fase 2: Análisis de las diferencias de configuración

Previamente identificadas las vulnerabilidades del servidor de prueba, se procederá a realizar la evaluación de las mismas con el fin de diseñar y proponer los procedimientos que permitan la mitigación del riesgo que conlleva contar con estas vulnerabilidades. Al tener el análisis terminado se procede a realizar la documentación del Manual de buenas prácticas, así como la documentación del trabajo de grado

B. Instrumentos o herramientas utilizadas

Para el desarrollo del proyecto se van a utilizar las siguientes herramientas que nos permiten detectar las vulnerabilidades en el Directorio Activo configurado en Windows Server 2012 R2

- Herramientas: Windows Server 2012

- Máquina Virtual (VirtualBox)
- OpenVas
- Nessus
- Microsoft Baseline Security Analizer
- Dcdiag

C. Población y muestra

Dado que el proyecto se realiza sobre un sistema operativo de prueba, no se ve la necesidad de trabajar con una población específica, sin embargo, se espera que el resultado del proyecto pueda ser asimilado y de buen uso por parte de los administradores de red.

D. Alcances y limitaciones

ALCANCE

El presente proyecto aplicado se encuentra entre los proyectos de Software inteligente y convergencia tecnológica, el cual tiene como fin identificar y evaluar las vulnerabilidades que atenten contra los principios fundamentales de la seguridad informática en el Directorio Activo en Windows Server 2012 R2, aportando mejores prácticas, medidas y procedimientos necesarios para mitigarlas.

Se desarrollará un Manual de buenas prácticas que recopile la configuración ideal establecida de acuerdo con el análisis de vulnerabilidades realizado

LIMITACIONES

Dentro del desarrollo del presente proyecto aplicado se pueden encontrar limitaciones como:

- El software Microsoft Baseline Security Analizer no viene en español se debe trabajar en Ingles.
- El sistema operativo Server 2012R2 tiene licencia de prueba por 90 días.

VI. PRODUCTOS A ENTREGAR

- Documento con pantallazos de paso a paso de instalación del Directorio Activo, escaneo para identificar vulnerabilidades.

Para poder realizar un escaneo es necesario instalar en un ambiente de pruebas el Directorio Activo en una máquina virtual con los requerimientos de hardware básicos para instalar el servicio del Directorio Activo en el Sistema Operativo Windows Server 2012R2.

- Documento con pantallazos de hallazgos encontrados

Cuando se realiza el escaneo de vulnerabilidades, este genera unos registros los cuales se muestran directamente desde la aplicación que se realizan en las máquinas virtuales instaladas tanto la que se va a escanear como la que se utiliza para realizar estos escaneos.

- Manual de buenas prácticas

Este Manual va a ser un documento de gran ayuda para los administradores de red que requieran implementar el Directorio Activo en una compañía, contiene la configuración avanzada para mitigar las vulnerabilidades encontradas en la presente investigación.

- Artículo

Este documento mostrará un acercamiento a la seguridad de la información desde la perspectiva del Directorio Activo, desde sus inicios, teniendo en cuenta como se define y como se aplica en diferentes ambientes haciendo énfasis en el Directorio Activo.

VII. ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

Teniendo en cuenta que la realización de un escaneo en un ambiente de pruebas se debe parametrizar de forma que permita escanear las vulnerabilidades, garantizando la virtualización del servidor que se va a escanear y el servidor Kalli Linux [26] desde el cual se ejecutaran las herramientas de escaneo.

La información plasmada en estos registros hace referencia a la configuración básica del Directorio Activo con algunos conceptos que no deben dejar pasar los administradores de red o personas encargadas de esta herramienta en una Compañía; Se puede afirmar que el Directorio Activo es una base de datos estructurada jerárquicamente, se debe tener en cuenta que para la configuración de un Directorio Activo lo primero es tener un dominio siendo su objeto principal, puede existir el directorio activo sin un subdominio y sin un bosque pero nunca sin un Dominio; Un dominio seria la representación lógica de una oficina, empresa o Unidad principal de un negocio dentro de este se crean los subdominios para organizar los usuarios pcs y servidores asignados a la compañía y tener claridad del cual es su Dominio Principal y subdominio con lo cual se prestara un mejor soporte y se identificaran los sitios de los dominios. La unión de dos subdominios es llamada bosque. Se debe tener en cuenta que para configurar un dominio se coloca una ip fija al servidor donde se va a instalar el Directorio Activo

A. AMBIENTE DE PRUEBAS

Definición: Un ambiente de pruebas es un término utilizado en el campo del software y desarrollo de sitios web previo a la producción. Describe la ubicación en la que se ven previamente los cambios en un sitio web o software y son ajustados antes de su publicación final.

Los ambientes de prueba pueden ser utilizados para actividades de pruebas de aceptación del usuario. Se suelen utilizar configuraciones de hardware similares a las del entorno de producción, con sujetos de prueba que proporcionan una previsión del rendimiento. Se creó un ambiente de pruebas para que esta investigación pueda ser aplicada en cualquier empresa que utilice Directorio Activo y no llegar a afectar algún servidor operativo.

Como se puede apreciar en la Figura 5 los sistemas de virtualización Virtual Box y Vmware son compatibles para este tipo de trabajos y configuraciones

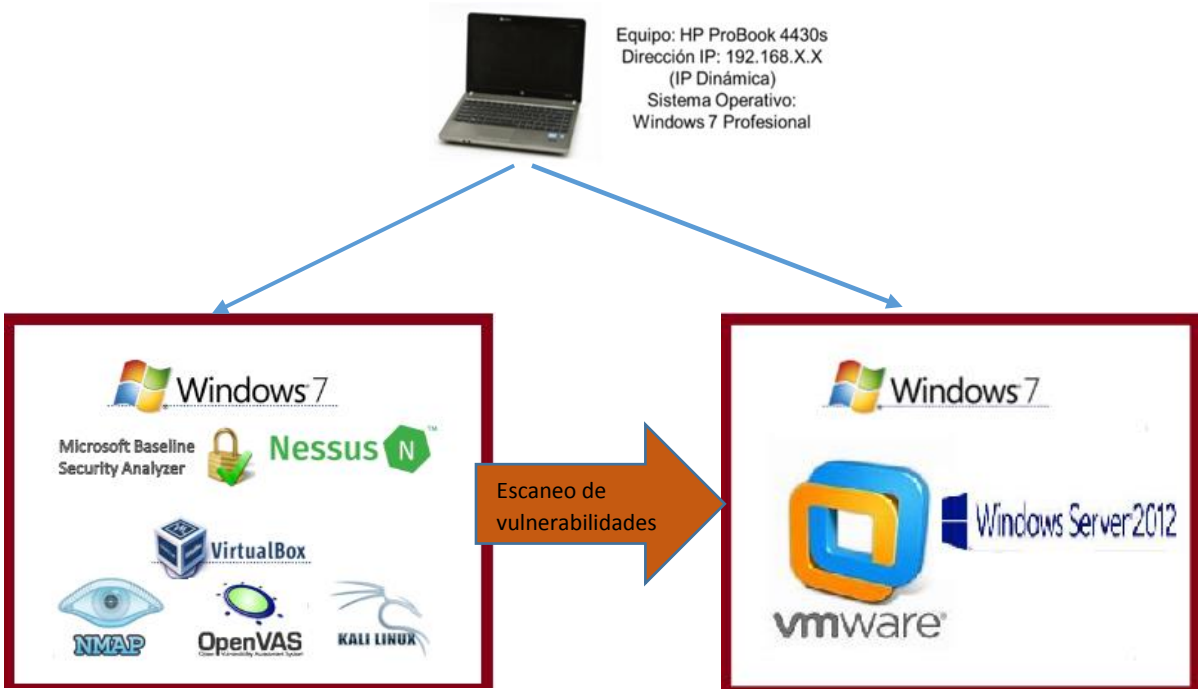

Figura 5. Ambiente de pruebas

Fuente Elaboracion propia apartir de la instalacion de Windows server 2012R2 [27]

En la gráfica anterior se evidencia que las herramientas de escaneo se pueden realizar desde el mismo servidor Linux configurándolas para subir sus servicios y actualizando los paquetes de instalación desde los repositorios de Linux .

B. REQUISITOS DE HARDWARE

En la siguiente tabla se plasman los requisitos para la instalación básica de las tres máquinas a utilizar:

CARACTERISTICAS	MAQUINA HOST	SERVER 2012 R2	KALLI LINUX
PROCESADOR	COREI5	1	2
NUMERO DE NUCLEOS	2 A 4	1	2
MEMORIA RAM	8 GB	2 GB	2
RED	Qualcomm Atheros AR9285 802.11b/g/n WiFi Adapter	BRIDGE DEFINIDA	BRIDGE DEFINIDA
CAPACIDAD EN DISCO	1 TERA	60 GB	61 GB
HIPERVISOR	N/A	VMWARE 9.0	VIRTUAL BOX
SISTEMA OPERATIVO	WINDOWS 7 PRO	WINDOWS 2012 R2	KALLI LINUX

Tabla 2. Requisitos de Hardware

Fuente elaboración propia a partir de la instalación de los servidores y virtualización.

En la tabla N° 2 se encuentra la descripción que contiene los recursos de la maquina física en la que se realiza la instalación.

C. REQUISITOS DE SOFTWARE

Para ejecutar los diferentes escaneos de vulnerabilidades se debe diseñar una correcta configuración y diseño del software requerido basados en el desarrollo del proyecto, se dispone la instalación y configuración de diferentes herramientas de distribución y código libre, con el fin de garantizar el mayor cubrimiento e identificación de las posibles vulnerabilidades existentes en el servidor, tabla 2 y 3.

SISTEMAS OPERATIVOS REQUERIDO PARA EL AMBIENTE DE PRUEBAS		
HERRAMIENTA	**VERSION**	**DESCRIPCION**
Windows 7	Professional – Service Pack 1	Este SO es el sistema empleado como anfitrión de los dos equipos que componen el ambiente de pruebas.
Windows Server	2012 R2- 64 Bits	El SO Windows Server 2012 R2 se instaló en una máquina virtual de Vmware.
Kali Linux	Versión 2017.2-amd64	Es sistema operativo se usó para instalar y ejecutar las herramientas, OpenVAS, NMAP y Microsoft Baseline Security Analyzer

Tabla 3. S.O Ambiente de pruebas

Fuente elaboración propia a partir de la instalación de Windows server 2012 R2 y virtualización

SOFTWARE PARA IMPLEMENTAR AMBIENTE DE PRUEBAS				
HERRAMIENTA	**A**	**B**	**VENTAJAS**	**DESVENTAJAS**
Interfaz Gráfica de Usuario de VirtualBox Version 6.0.12 r133076 (Qt5.6.2) Copyright © 2019 Oracle Corporation and/or its affiliates. All rights reserved"	X	X	❖ Es una herramienta multiplataforma compatible con Windows, macOS, Linux y Solaris. ❖ Puede controlarse a través de símbolo de sistema. ❖ Cuenta con herramientas especiales para compartir archivos entre máquinas. ❖ Permite crear instantáneas para restaurar el estado anterior de una VM fácilmente. ❖ Soporte limitado para gráficos 3D. ❖ Permite utilizar aplicaciones virtualizadas como si se trataran de aplicaciones del sistema «separándolas». ❖ Es compatible con las máquinas virtuales de VMware. ❖ Cuenta con una herramienta de captura de vídeo.	❖ El sistema anfitrión debe ceder recursos como espacio en disco duro, memoria RAM o número de procesadores a los sistemas operativos emulados en la máquina virtual. ❖ Requiere de un equipo informático potente y con gran rendimiento, de manera que pueda soportar los procesos de dos o más sistemas operativos al tiempo.
Nessus Vulnerability Scanner versión 6.11.1 de 64 bits	X		❖ Define el nivel de las vulnerabilidades (critica, alta, media, baja e informativa ❖ Gran cantidad de plugins para el análisis ❖ Rapidez en términos de tiempo en sus escaneos. ❖ Puede hacer escaneos sobre aplicaciones web. ❖ Herramienta fácil de usar y práctica.	❖ Para acceder a todas sus funciones se debe contar con una versión paga.
Open Vas	X	X	❖ Herramienta gratuita ❖ No tiene un límite de direcciones IP en sus escaneos ❖ Puede hacer escaneos sobre aplicaciones web	❖ Complejidad de instalación y configuración ❖ Poca cantidad de plugins. ❖ No detecta vulnerabilidades críticas.
NMAP		X	❖ Es una herramienta de código abierto. ❖ Multiplataforma ❖ Realiza escaneos que arroja resultados ❖ que no pueden ser detectados a simple ❖ vista por un usuario o administrador de ❖ red. ❖ Detecta puertos abiertos, cerrados, ❖ información sobre sistema operativo. ❖ Identifica que computadoras están ❖ conectadas a una red. ❖ Lista los servicios que se ejecutan en una ❖ máquina.	❖ Escanea solo una IP al tiempo. ❖ De acuerdo la complejidad del tipo de escaneo, este tardara. ❖ La velocidad del escaneo está sujeta a la capacidad de rendimiento del equipo donde se está ejecutando.
Microsoft Baseline Security Analyzer 2.3	X		❖ Herramienta gratuita. ❖ Permite mejorar los procesos de administración en la seguridad informática. ❖ Detecta errores de configuración de seguridad y de actualización de seguridad. ❖ Compatible con todas las plataformas de Windows. ❖ Realiza el análisis de las contraseñas de las cuentas de usuario e indica si estas son vulnerables. ❖ Analiza el servidor IIS. ❖ Analiza las bases de datos	❖ Solo puede ser ejecutada en sistemas operativos Windows. ❖ Su funcionalidad está enfocada hacia las pymes. ❖ Requiere que quien administre la herramienta tenga conocimiento avanzado en redes y administración de sistemas operativos Windows. ❖ No está disponible en español

Tabla 4 . Software Ambiente de pruebas

Convenciones: A: Equipo Evaluador B: Equipo Evaluado

Fuente: Elaboración propia a partir de la instalación de Windows server y virtualización

D. *INSTALACIÓN DE WINDOWS SERVER 2012 R2 Y VMWARE*

Para el ambiente de pruebas del equipo que será evaluado en búsqueda de vulnerabilidades de seguridad, se instaló el software de virtualización Vmware Version 9.0.1 build-894247 y se creó una máquina virtual para la instalación del sistema operativo Windows server 2012 R2 en su versión de 64 bits, teniendo en cuenta el adaptador de red con la opción Adaptador puente para permitir la comunicación con la maquina evaluada, esto es posible apreciarlo en la figura 5.

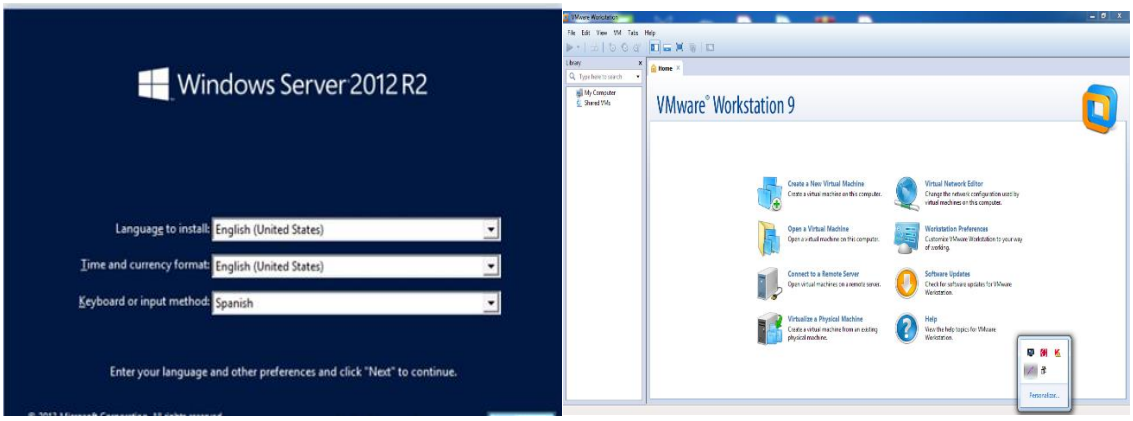

Figura 5. Instalación y configuración vmware-wserver 2012R2

Fuente elaboración propia a partir de la instalación

Para profundizar en esta instalación y configuración revisar Anexo 1 Anexo1 Instalacion Windows Server 2012 y Vm Ware.

Una vez instalados este servidor queda completamente operativo para realizar el escaneo de vulnerabilidades

E. *CONFIGURACIÓN DE AMBIENTE DE PRUEBAS*

En la figura 5 se evidencia que para la configuración del ambiente de pruebas se utilizó el software VirtualBox versión 6.0 el cual permite la creación de máquinas virtuales bajo el entorno del sistema operativo Windows 7 SP1, con el fin de realizar prácticas sobre otros sistemas sin afectar

el sistema host, hecho esto se configuran las máquinas virtuales necesario en el desarrollo del proyecto.

Instalación del software de virtualización – VirtualBox

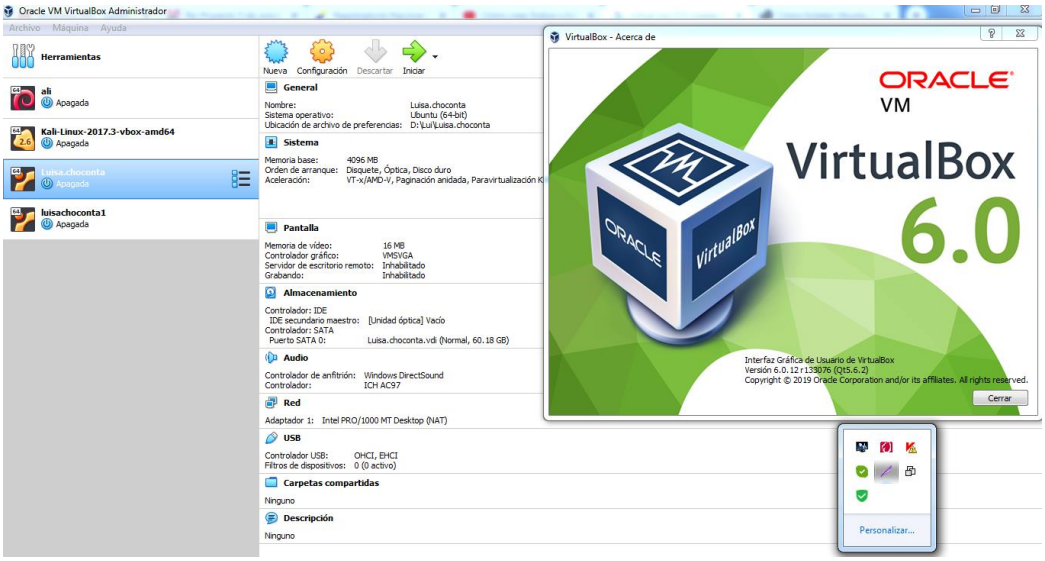

Figura 6. Instalación Virtual box

Fuente elaboración propia a partir de la instalación.

F. *INSTALACIÓN KALLI LINUX*

Kalli Linux es una distribución basada en debían, diseñada para la auditoria de seguridad, los tests de intrusión y la informática forense en esta herramienta son de gran ayuda para esta investigación ya que con sus paquetes y distribuciones que están disponibles para las diferentes arquitecturas de los sistemas operativos, permiten cumplir con los objetivos de escaneo para realizar las pruebas de vulnerabilidades ; incluye más de 600 aplicaciones para auditoria, seguridad e informática forense; incluyendo escáneres de puertos, suites de crackeo wi-fi , suite para construir troyanos y programas para descubrir clases. [28]

Como se puede apreciar en la figura 7 Se realiza la importación de la máquina de Kalli Linux [29] la cual viene con Nessus configurado previamente para utilizarlo para realizar el escaneo.

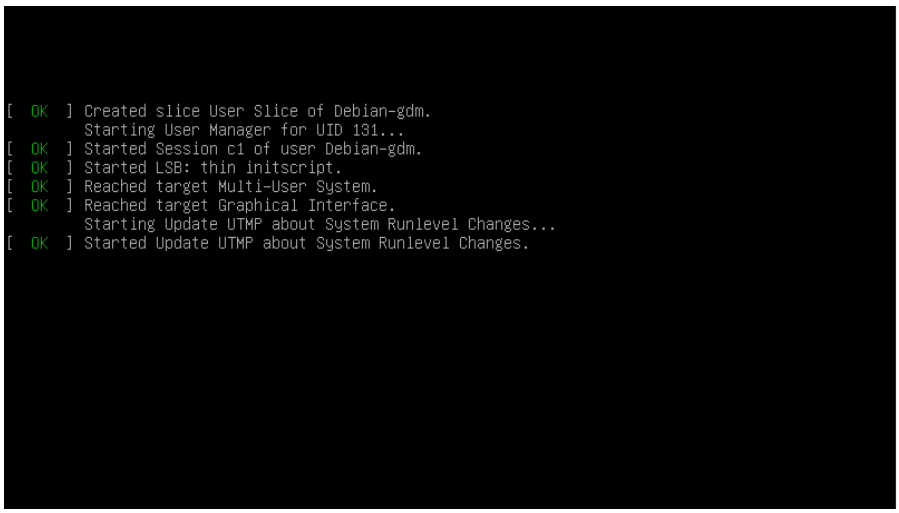

Figura 7. Importación maquina Kalli Linux

Fuente elaboración propia a partir de la instalación

G. *INSTALACIÓN Y CONFIGURACIÓN NESSUS VULNERABILITY*

Para identificar las vulnerabilidades que posee el Directorio Activo, se ejecutara uno de los escaneos de vulnerabilidades usando la aplicación Nessus Vulnerability Scanner, [30] esta es una aplicación web que permite la identificación de vulnerabilidades en una amplia gama de sistemas operativos. Nessus logra identificar las vulnerabilidades y riesgos que estas conllevan usando un daemon, el cual ejecuta el escaneo en el sistema y/o equipo objetivo, luego Nessus cliente (Este hace referencia a la aplicación de interfaz gráfica) muestra el avance e informa sobre el estado del escaneo.

Con NESSUS se intenta comprobar si son vulnerables o no los servicios que están ejecutándose, por lo tanto hay que tener mucho más cuidado con este programa, ya que se puede rozar el lımite entre lo permitido y lo no permitido si se escanean máquinas que estén dentro de la red, y de la misma forma, si están dentro del dominio, como si no, debemos tener en cuenta que es posible que la prueba de vulnerabilidades puede provocar una denegación de servicio contra la maquina escaneada [31].

Al realizar una evaluación de vulnerabilidad usando Nessus se encuentran errores de programación que permitan a los intrusos obtener acceso no autorizado. Tiene una interfaz muy

amigable ya que permite modificar las pestañas y preferencias siendo estas configurables y adaptables para diferentes ambientes de acuerdo a la necesidad, es un escáner en tiempo real teniendo en cuenta que prioriza las vulnerabilidades administrándolas según su criticidad y entregando informes de denegación de servicio y fugas de información con falsos positivos entre pruebas intrusivas y no intrusivas, teniendo en cuenta la topología escanea toda la red de la compañía según se requiera [32].

Para ello se descarga la aplicación Nessus Versión 6.11.1 de 64 bits la cual es compatible con sistema operativos Microsoft Windows (Servidor 2012, Servidor 2012 R2, 7, 8, 10, 2016).

En la figura 9 se realizará por medio de comandos la inicialización del servicio de Nessus escáner en Kalli Linux

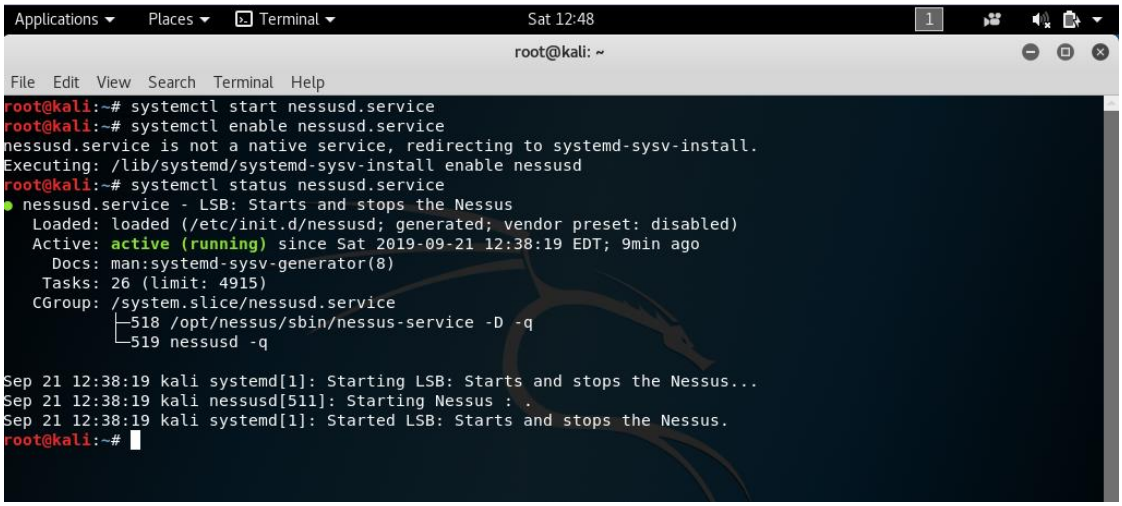

Figura 8. Configuracion de Nessus

Fuente elaboración propia a partir de la instalación

Al dar inicio a los servicios por medio de los comandos en Kalli Linux se abre la interfaz de Nessus como se aprecia en la figura 9 se puede ver la interfaz gráfica de Nessus para comenzar con el escaneo del servidor

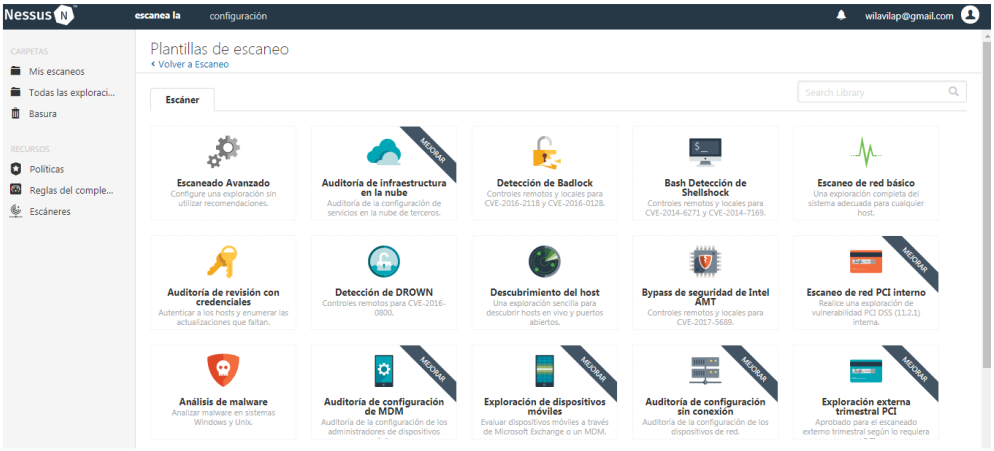

Figura 9. Interfaz de Escaneo Nessus

Fuente elaboración propia a partir de la instalación

Para realizar el escaneo de vulnerabilidades se deben ingresar los siguientes parámetros: El nombre del escaneo el cual puede ser "Escaneo vulnerabilidades servidor", una breve descripción del mismo, la carpeta donde se guardará la información y la dirección IP de la maquina a escanear, ver Figura 10.

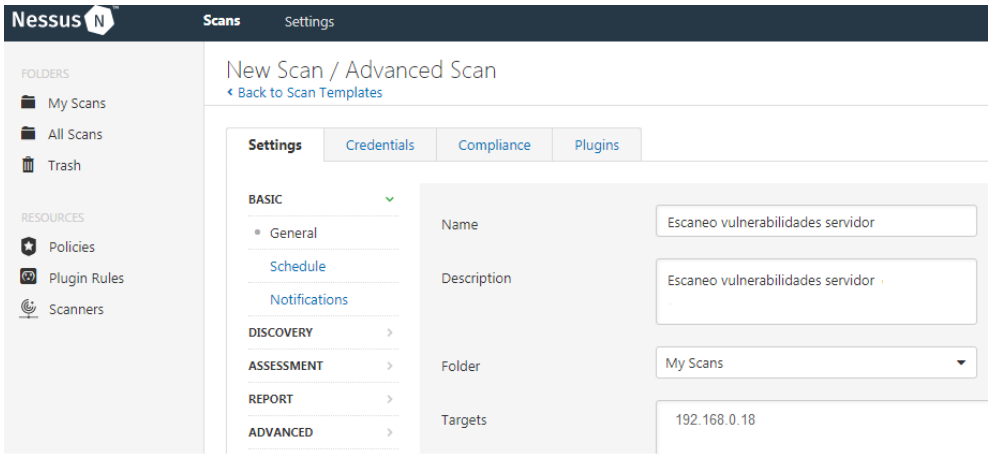

Figura 10.Configuracion Nessus de servidor a escanear

Fuente: elaboración propia a partir de la instalación

Una vez terminado el escaneo, Nessus genera el reporte de las vulnerabilidades encontradas en el servidor, el cual es indispensable para la ejecución de la fase 2 del proyecto.

Para evidenciar el escaneo de esta herramienta ver el anexo 2. (Anexo 2_Escaner Nessus)

H. *ESCANEO DE VULNERABILIDADES CON OPEN VAS*

Open Vas es un framework que tiene como base servicios y herramientas para la evaluar vulnerabilidades y puede utilizarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM (Open Source Security Information Management).

En la máquina de Kali Linux ya se cuenta con esta herramienta instalada como predeterminada pero se debe subir el servicio, puede ser utilizada a través de dos interfaces, desde línea de comandos (OpenVAS CLI) o una interfaz web (Greenbone Security Assistant). Una vez instalada en el sistema, también puede utilizarse desde Metasploit, el framework para la explotación de vulnerabilidades.

Por medio de las interfaces se actúa de manera recíproca con estos dos servicios: OpenVAS Manager y OpenVAS Scanner. El gestor es el servicio que tiene a su cargo labores como el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios (incluyendo grupos y roles) [33]

De manera simultánea, el escáner realiza las denominadas pruebas de Vulnerabilidades de red (NVT Network Vulnerability Tests), formadas por rutinas que comprueban la aparición de un problema de seguridad específico conocido o potencial en los sistemas.

El proyecto OpenVAS conserva una colección de NVT (OpenVAS NVT Feed) que aumenta continuamente y actualiza los registros periódicamente. Los equipos instalados con OpenVAS se sincronizan con los servidores para actualizar las pruebas de vulnerabilidades [34]

Para realizar el escaneo de vulnerabilidades con OpenVas se debe iniciar en Kalli Linux el Servicio para ingresar a la configuración por la interfaz web Figuras 11 y 12.

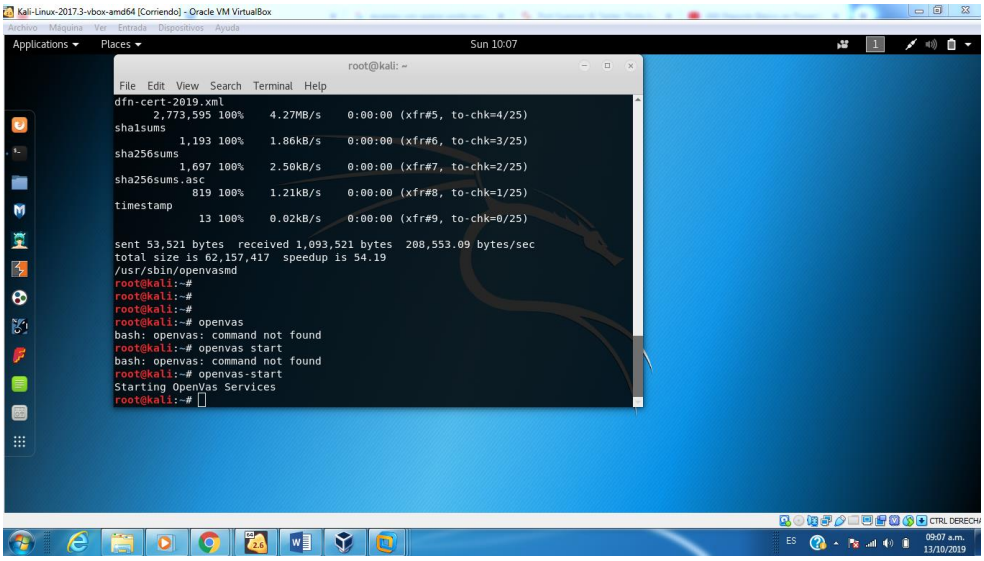

Figura 11. Configuración OpenVas

Fuente propia a partir de la instalación

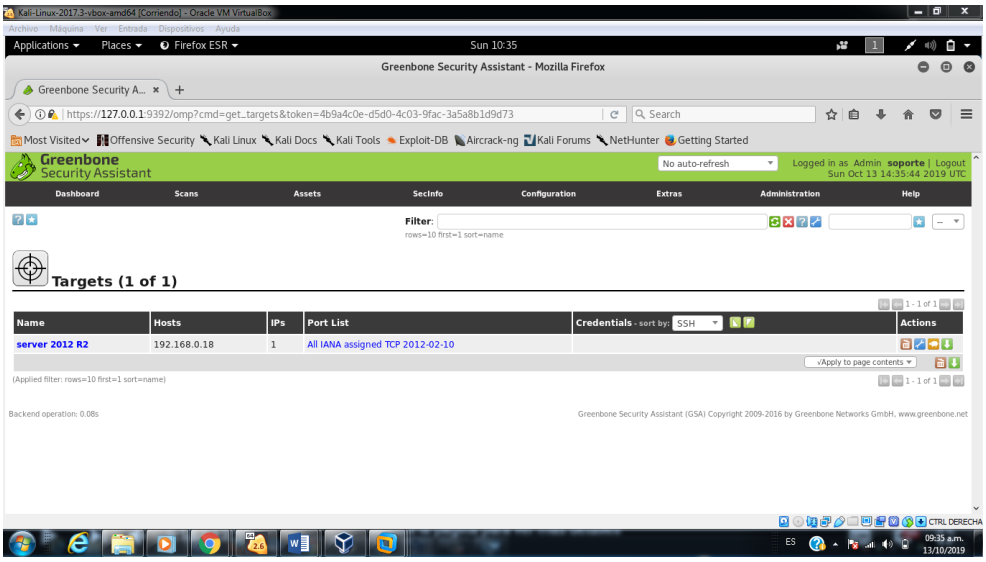

Figura 12. Interfaz web OpenVas

Fuente propia a partir de la instalación

Luego de realizar el escaneo OpenVas genera un informe detallado de las vulnerabilidades con nombre y gráficos del mismo como se puede apreciar en la figura 13 y 14

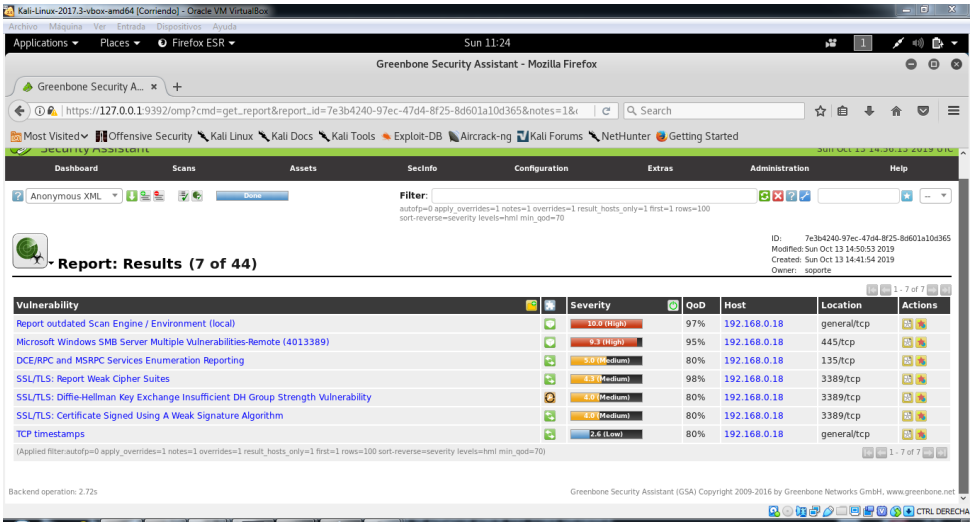

Figura 13. Resultado de escaneo Reporte

Fuente propia a partir de la instalación

Figura 14. Resultado de escaneo en forma grafica

Fuente propia a partir de la instalación

Para ampliar esta información ver Anexo 3 Escaneo de vulnerabilidades OpenVas.

Con los resultados generados anteriormente se verifican las vulnerabilidades las cuales se tienen en cuenta en el manual de buenas prácticas.

I. *VULNERABILIDADES DETECTADAS CON MICROSOFT BASELINE SECURITY ANALYZER*

Microsoft Baseline Security Analyzer (MBSA) es una herramienta gratuita desarrollada por Microsoft para que las pymes conozcan sus vulnerabilidades en cuanto a seguridad informática se refiere; se instala en sistemas operativos Microsoft, sea Windows o Windows Server, así como otras aplicaciones de servidor de Microsoft como Exchange.

Algunas de sus funciones son:

- Check Windows for administrative vulnerabilities: Al habilitar esta opción, MBSA analizará el equipo en búsqueda de vulnerabilidades por parte de los administradores del sistema (cuentas administrativas)
- Check for weak passwords: Esta opción analiza los passwords de las cuentas de usuarios e identifica passwords que son fáciles de descifrar
- Check for IIS administrative vulnerabilities: Aanaliza el servidor IIS (si se encuentra instalado)
- Check for SQL administrative vulnerabilities: Con esta opción habilitada, MBSA analizará nuestra base de datos SQL en busca que debilidades en seguridad.
- Check for security updates: Al habilitar esta opción, el sistema buscará actualizaciones en línea para el sistema operativo.

Esta herramienta es capaz de realizar análisis sencillos de vulnerabilidades en infraestructuras informáticas de empresas pequeñas, las cuales han estado sufriendo ataques informáticos o infección por virus y no se ha podido determinar la causa exacta de por donde se están produciendo. Por ende, para su uso, se requiere de conocimiento técnico en redes y administración de Windows, por lo que su uso es para el personal del TI dentro de la empresa. Así mismo, está claro que esta herramienta no remplaza a un software de seguridad corporativo (como los antivirus y suite de seguridad de tipo corporativo de los principales fabricantes).

Como es de aclarar los resultados que entregue MBSA no indican al 100% los motivos por los cuales se puede estar sufriendo un ataque o incidente de seguridad informática, detectar infección

por virus o gusanos; pero es un muy buen complemento para reforzar aquellos puntos frágiles en la seguridad TI que no se han tenido en cuenta.

Se puede apreciar en la Figura 16 que su configuración es básica después de instalarlo se coloca la ip del equipo o el nombre del equipo a escanear

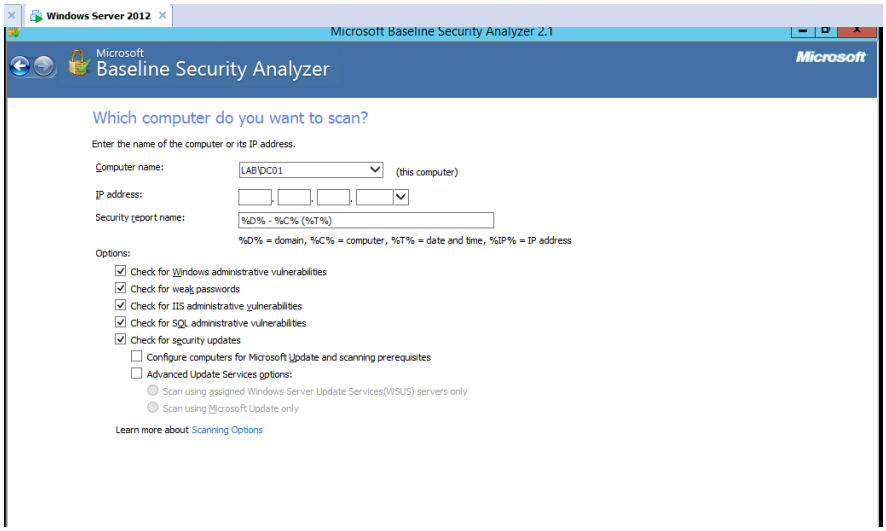

Figura 15. Configuración de MBSA

Fuente propia a partir de la instalación

Ya realizada esta configuración el arroja los resultados de las vulnerabilidades en este caso fueron 10 clasificadas en Riesgo Critico, Medio y Bajo la cual se puede ver en la gráfica 16.

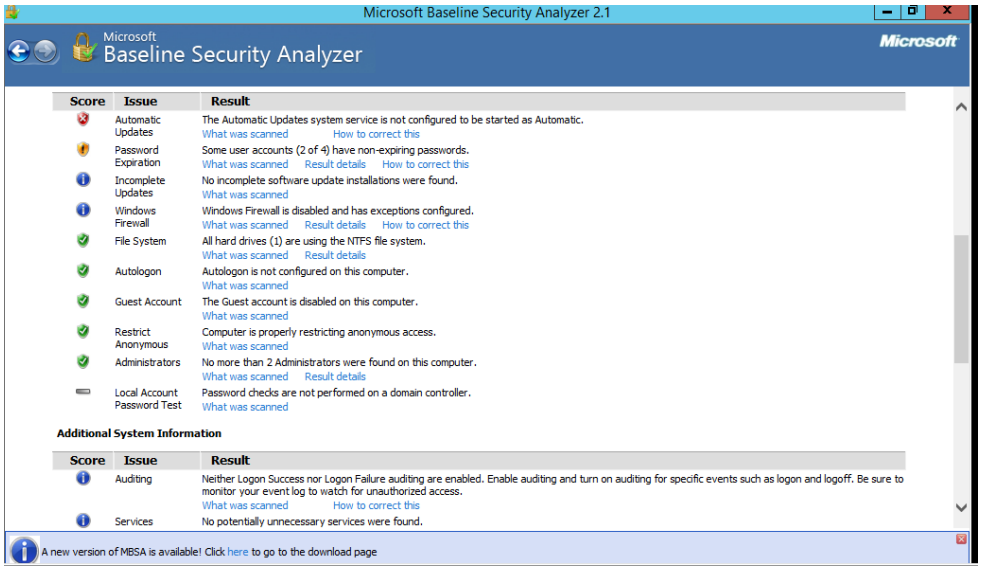

Figura 16. Resultado de vulnerabilidades MBSA

Fuente propia a partir de la instalación

Con esta herramienta se tiene un mejor control en el caso de las actualizaciones lanzadas por Microsoft y un seguimiento de las mismas para mantener los equipos actualizados y así cerrar brechas de seguridad para los atacantes informáticos y ciberdelincuentes [35]

J. *ANALISIS AL CONTROLADOR DE DOMINIO CON DCDIAG*

Dcdiag es una utilidad de línea de comandos de Microsoft Windows que puede analizar el estado de los controladores de dominio en un bosque o empresa. Puede elegir analizar un solo controlador de dominio o todos los DC en un bosque la cual puede encontrar problemas entre varios controladores de dominio tiene un total de 30 pruebas diferentes, y algunas pruebas tenían múltiples pruebas. Al ejecutar este comando se puede ver una lista de pruebas en el menú de ayuda de comandos, ejecute dcdiag /? para ver el menú de ayuda.

Para ejecutar esta herramienta es solo colocarla en el CMD del servidor y este arrojará un análisis completo del Directorio Activo, no necesariamente los errores que arroje se debe a mala configuración, sino que también hace referencia a configuraciones y registros del mismo.

Ver Anexo 4 (Reporte DCDiag).

VIII. CONCLUSIÓNES

Con la realización del presente proyecto, la investigación realizada, las pruebas que en los anexos se adjuntan y el manual de buenas prácticas que hacen parte del mismo, se puede concluir que:

1. La minimización de las vulnerabilidades en la configuración del Directorio Activo es necesaria para los administradores de red en el momento de tener a cargo la infraestructura de una compañía y estar definiendo los grupos, usuarios y políticas locales ya que al no quedar con las correctas reglas y revisiones se arriesga tener eventos catastróficos.
2. La evaluación realizada por las compañías en cuanto a seguridad tiene una visibilidad limitada del estado real de su infraestructura de TI y esto con lleva a que se presenten vulnerabilidades que exponen toda la red a un riesgo y al realizar una configuración robusta nos cierra estas brechas de seguridad. Con esta investigación
3. El manual de buenas prácticas debe constituirse en una herramienta para el área de TI las compañías al momento de realizar la configuración del Directorio Activo, ya que en el se describe el paso a paso previo a una investigación realizada para preveer y atacar desde su inicio las posibles amenazas que por desconocimiento se cometen en una configuración de Directorio Activo.

REFERENCIAS

[1] paologm, «https://paologmcom.wordpress.com/2016/11/20/1-1-principios-de-la-seguridad-informatica/,» 20 11 2016. [En línea]. Available: https://paologmcom.wordpress.com/2016/11/20/1-1-principios-de-la-seguridad-informatica/. [Último acceso: 12 05 2019].

[2] R. Romero, Sistemas operativos en red,, Madrid: Macmillan Iberia, S.A, 2013.

[3] B. J. F. Roa, Seguridad Informatica, España : McGraw-Hill, 2013.

[4] C. R. Carceller, Servicios en red, Madrid: ProQuest Ebook Central., 2013.

[5] S. d. l. Santos, «http://www.globalgate.com.ar,» Globalgate, [En línea]. Available: http://www.globalgate.com.ar/novedades-grave-vulnerabilidad-que-afecta-a-entornos-con-ad--active-directory.html. [Último acceso: 12 Mayo 2019].

[6] Tecnosfera, «El tiempo.com,» Tecnosfera, 17 Septiembre 2017. [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370. [Último acceso: 12 Mayo 2019].

[7] El tiempo.com, «https://www.eltiempo.com,» [En línea]. Available: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370.

[8] Panda, «Panda Security,» 2018. [En línea]. Available: https://www.pandasecurity.com/spain/mediacenter/seguridad/datos-evolucion-ciberamenazas-en-2018/. [Último acceso: 5 Mayo 2019].

[9] Y. D. a. D. L. S. Thomas W. Shinder, Windows Server 2012 Security from End to Edge and Beyond, Amsterdan Paises bajos: elseiver inc, 2013.

[10] J. W. &. Sons, MCSA Windows Server 2012 R2 Installation and Configuration Study Guide, Estados Unidos: John Wiley & Sons, 2015.

[11] N. Bonnet, Windows Server 2012 R2 - Administración: Preparación para la certificación MCSA, España: Eni, 2015.

[12] T. Denoeux, «Array,» *Array,* 2019.

[13] J. F. G. Albacete, Seguridad en equipos informaticos, ANTEQUERA Malaga: IC Editorial, 2014.

[14] R. M. R. S. J. R. Gema Escrivá Gascó, Seguridad informática, MacMillan Iberia S.A, 2013, p. 15.

[15] Á. G. Vieites, Enciclopedia de la Seguridad Informática. 2ª edición, Grupo Editorial RA-MA, , 2011, p. 830 páginas.

[16] M. A. F. Rosa, Windows Server 2012 R2, Peri Miraflores: Macro, 2014.

[17] Windows Server 2012 Informatica Tecnica, Barcelona: Eni, 2014.

[18] P. AG, «Paessler,» 2017. [En línea]. Available: https://www.es.paessler.com/it-explained/active-directory. [Último acceso: 1 10 2019].

[19] Microsoft, «support.microsoft.com,» [En línea]. Available: https://support.microsoft.com/es-co/help/300684/deployment-and-operation-of-active-directory-domains-that-are-configur. [Último acceso: 22 09 2019].

[20] W. R. Stanek, Windows Server 2012: Gua del administrador, Madrid España: Anaya Multimedia, 2013.

[21] A. Binduf, H. Othman y B. Hanan, «Active Directory and Related Aspects of,» 2018. [En línea].

[22] F. G. d. l. Nacion, 2019. [En línea]. Available: www.fiscalia.gov.co/colombia/seccionales/capturadas-121-personas-por-delitos-. [Último acceso: 8 Mayo 2019].

[23] M. Wataru, M. Fujimoto y T. Mitsunaga, «Detecting APT attacks against Active Directory,» 2018. [En línea]. Available: Conference on Applications, Information and Network Security (AINS). [Último acceso: 1 10 2019].

[24] Chih-Hung Hsieh y . L. Chia-Min, «Anomaly Detection on Active Directory Log,» 2015. [En línea]. [Último acceso: 15 09 2019].

[25] Microsoft, «Arquitectura de Active Directory,» 2017. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727030(v=technet.10)?redirectedfrom=MSDN. [Último acceso: 01 10 2019].

[26] C. ©. 2. S. o. T. l. d. reservados., «Kali.org,» Copyright © 2019 Seguridad ofensiva. Todos los derechos reservados., 2019. [En línea]. Available: https://es.docs.kali.org/kali-policy-es/politica-de-codigo-abierto-en-kali-linux. [Último acceso: 15 09 2019].

[27] I. P. Colombia, «blogs.technet.microsoft.com/,» 02 2015. [En línea]. Available: https://blogs.technet.microsoft.com/itprocol/2015/08/11/101-cosas-que-puedes-hacer-con-cloud-os-cosa-4/. [Último acceso: 10 06 2019].

[28] D. S. Orcero, Kalli Linux, España: Ra-Ma, 2018.

[29] M. P. Sanz, Seguridad en Linux, Madrid: Editorial Universidad Autónoma de Madrid, 2008.

[30] M. G. a. G. P. P. P. Álvarez, Seguridad informática para empresas y particulares, España: McGraw-Hil, 2004.

[31] M. P. Sanz, Seguridad en Linux; guia practica, España: Editorial Universidad Autonoma de Madrid, 2008, p. ProQuest ebook Central.

[32] R. Rogers, Nessus Network Auditing 2 Ed, Syngress, 2008.

[33] K. B. J. C. Michael T. Simpson, Hands-On Ethical Hacking and Network Defense, Boston: Cengage Learning, 2010.

[34] M. Á. Mendoza, «Cómo utilizar OpenVAS para la evaluación de vulnerabilidades,» 18 Noviembre 2014. [En línea]. Available: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/. [Último acceso: 25 09 2019].

[35] B. J. F. Roa, «Seguridad informática,» España, McGraw-Hill, 2013, pp. 12,18,21.

[36] Universidad Autónoma de MAdrid, «Citas y elaboración de bibliografía: el plagio y el uso ético de la información: Estilo IEEE,» 26 07 2019. [En línea]. Available: https://biblioguias.uam.es/citar/estilo_ieee. [Último acceso: 29 07 2019].